JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

P. LLORENTE

E. NART

N. VILA

Decomposition of primes in number fields defined by trinomials

Journal de Théorie des Nombres de Bordeaux 2e série, tome 3, nº 1 (1991), p. 27-41

<http://www.numdam.org/item?id=JTNB_1991__3_1_27_0>

© Université Bordeaux 1, 1991, tous droits réservés.

L'accès aux archives de la revue « Journal de Théorie des Nombres de Bordeaux » (http://jtnb.cedram.org/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme Numérisation de documents anciens mathématiques

http://www.numdam.org/

Séminaire de Théorie des Nombres,
Bordeaux **3** *(1991), 27-41*

Decomposition of primes in number fields defined by trinomials.

par P. LLORENTE, E. NART AND N. VILA

Abstract — *In this paper we deal with the problem of finding the prime-ideal decomposition of a prime integer in a number field K defined by an irreducible trinomial of the type $X^{p^m} + AX + B \in \mathbb{Z}[X]$, in terms of A and B. We also compute effectively the discriminant of K.*

1. Introduction

Let K be the number field defined by an irreducible trinomial of the type :

$$X^{p^m} + AX + B, \quad A, B \in \mathbb{Z}, \quad p \text{ prime}, \ m \geq 1.$$

In this paper we study the prime-ideal decomposition of the rational primes in K. Our results extend those of Vélez in [6], where he deals with the decomposition of p in the case $A = 0$. However, the methods are different, ours being based on Newton's polygon techniques. The results are essentially complete except for a few special cases which can be handled by an specific treatment (see section 2.3). This is done explicitely for $p^n = 4$ or 5, so that there are no exceptions at all for quartic and quintic trinomials.

Let us remark that the main aim of the paper is to give a complete answer in the case $p|A, p \nmid B$ (Theorems 3 and 4). The results concerning the other cases are easily obtained applying the ideas of [2], where we dealt with the computation of the discriminant of K, whereas the case $p|A, p \nmid B$ was not even considered. We give also the p-valuation of the discriminant of K in all cases including those not covered by [2].

Mots clefs: Decomposition of primes, Discriminant, Trinomials..
Manuscrit reçu le 20 juillet 1990 .

2. Results

Let $K = \mathbb{Q}(\theta)$, where θ is a root of an irreducible polynomial of the type :

$$f(X) = X^n + AX + B,$$

where $n, A, B \in \mathbb{Z}, n > 3$. For the case $n = 3$ see [1]. Let us denote by d and

$$D = (-1)^{\frac{n(n-1)}{2}}(n^n B^{n-1} + (-1)^{n-1}(n-1)^{n-1}A^n),$$

the respective discriminants of K and θ. For simplicity we shall write in the sequel N for the ideal norm $N_{K/\mathbb{Q}}$.

For any prime $q \in \mathbb{Z}$ and integer $u \in \mathbb{Z}$ (or q-adic integer $u \in \mathbb{Z}_q$) we shall denote by $v_q(u)$ the greatest exponent s such that $q^s | u$ and we shall write $u_q := u/q^{v_q(u)}$.

It is well-known that we can assume that the conditions :

$$v_q(A) \geq n-1, \quad v_q(B) \geq n,$$

are not satisfied simultaneously for any prime integer q. We shall make this assumption throughout the paper.

Let $F(X) \in \mathbb{Z}[X]$ be a polynomial, $q \in \mathbb{Z}$ a prime integer and let

$$F(X) \equiv \Phi_1(X)^{e_1} \cdot \cdots \cdot \Phi_s(X)^{e_s} \pmod{q},$$

be the decomposition of $F(X)$ as a product of irreducible factors (mod q). An integer ideal $\mathfrak{a}$ of any number field L will be called "*q analogous to the polynomial $F(X)$*" if the decomposition of $\mathfrak{a}$ into a product of prime ideals of L is of the type :

$$\mathfrak{a} = \mathfrak{q}_1^{e_1} \cdot \cdots \cdot \mathfrak{q}_s^{e_s}, \quad N_{L/\mathbb{Q}}(\mathfrak{q}_i) = q^{deg(\Phi_i(X))} \text{ for all } i.$$

2.1. Decomposition of the primes q not dividing n.

THEOREM 1. *Let $q \in \mathbb{Z}$ be a prime number such that $q \nmid n$. Let us denote $a = (n-1, v_q(A))$ and $b = (n, v_q(B))$. The decomposition of q into a product of prime ideals of K is a follows :*

If $v_q(B) > v_q(A)$ and $q \nmid a$,

(2.1.1) $\quad q = \mathfrak{q}\mathfrak{a}^{(n-1)/a}, \; N(\mathfrak{q}) = q, \; \mathfrak{a} \quad q-$ *analogous to* $X^a - A_q$.

If $v_q(B) \leq v_q(A)$ *and* $v_q(A) > 0$,

$$q = \mathfrak{a}^{n/b},\ \mathfrak{a}\quad q-\textit{analogous to } X^b - B_q. \tag{2.1.2}$$

If $q \not| AB$ *and* $q|D$, *the decomposition of* $f(X)$ *into a product of irreducible factors (mod* q*) is of the type :*

$$f(X) \equiv (x-u)^2.\Phi_1(X)\cdot \cdots \cdot \Phi_s(X) \pmod q, \tag{2.1.3}$$

and we have

$$q = \mathfrak{q}_1 \cdot \cdots \cdot \mathfrak{q}_s.\mathfrak{a},\ N(\mathfrak{q}_i) = q^{deg(\Phi_i(X))} \textit{ for all } i,\ \ N(\mathfrak{a}) = q^2, \tag{2.1.4}$$

where

$$\mathfrak{a} = \begin{cases} \mathfrak{q}.\mathfrak{q}',\ N(\mathfrak{q}) = N(\mathfrak{q}') = q, \textit{ if } v_q(D) \textit{ even and } \left(\frac{D_q}{q}\right) = (-1)^{n-s} \\ \mathfrak{q},\ N(\mathfrak{q}) = q^2, \textit{ if } v_q(D) \textit{ even and } \left(\frac{D_q}{q}\right) = (-1)^{n-s+1} \\ \mathfrak{q}^2,\ N(\mathfrak{q}) = q, \textit{ if } v_q(D) \textit{ odd.} \end{cases}$$

If $q \not| ABD$, q *is* q*-analogous to* $f(X)$. (2.1.5)

$$v_q(d) = \begin{cases} n-1-a+\inf\{(n-1)v_q(B) - nv_q(A), (n-1)v_q(n-1)\}, \\ \qquad\qquad if\ \ v_q(B) > v_q(A) \textit{ and } q \not| a, \\ n-b, \quad if\ \ v_q(B) \leq v_q(A) \textit{ and } v_q(A) > 0, \\ 0, \qquad if\ \ q \not| AB \textit{ and } v_q(D) \textit{ even}, \\ 1, \qquad if\ \ q \not| AB \textit{ and } v_q(D) \textit{ odd}. \end{cases}$$

2.2. Decomposition of the primes p dividing n

THEOREM 2. *If* $p \not| A$, *then* p *is* p*-analogous to* $f(X)$ *and* $v_p(d) = 0$.
If $v_p(B) > v_p(A) > 0$, *then*

$$p = \mathfrak{a}^{(n-1)/a}\mathfrak{p},\quad \mathfrak{a}\ \ p-\ \textit{analogous to } X^a + A_p,\ N(\mathfrak{p}) = p$$

and $v_p(d) = n - a - 1$, *where we have denoted* $a = (n-1, v_p(A))$.

If $0 < v_p(B) \leq v_p(A)$ *and* $p \not| v_p(B)$,
$p = \mathfrak{p}^n, N(\mathfrak{p}) = p$ *and* $v_p(d) = n - 1 + \inf\{nv_p(A) - (n-1)v_p(B), nm\}$.

From now on we assume that $n = p^m > 3$ for some prime $p \in \mathbb{Z}$ and integer $m \geq 1$.

THEOREM 3. *Suppose that* $p > 2$, $p|A$ *and* $p \not| B$. *Let us denote :*
$r_0 = v_p(f(-B))$, $r_1 = v_p(f'(-B))$, $r = \inf\{m+1, r_1, r_0\}$, $s_0 = v_p(D) - mn$;
$e = p^{m-r+1}$, $e_k = p^{m-k}(p-1)$, $1 \le k < m$, $e_m = p-2$; $J = (n-e)/(p-1)$,
$I = \frac{1}{2}(v_p(D) - v_p(d))$.

Then we have :

$$(2.2.1) \quad p = \begin{cases} \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_{r-1}^{e_{r-1}}.\mathfrak{a}, & N(\mathfrak{p}_k) = p \ \textit{for all} \ k, \ \textit{if} \ r \le m, \\ \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_{m-1}^{e_{m-1}}.\mathfrak{b}, & N(\mathfrak{p}_k) = p \ \textit{for all} \ k, \ \textit{if} \ r = m+1, \end{cases}$$

where

$$\mathfrak{a} = \begin{cases} \mathfrak{p}^e, & N(\mathfrak{p}) = p, \ \textit{if} \ r_0 \le r_1, & (2.2.2) \\ \mathfrak{p}^{e-1}.\mathfrak{p}', & N(\mathfrak{p}) = N(\mathfrak{p}') = p, \ \textit{if} \ r_0 > r_1. & (2.2.3) \end{cases}$$

If $p = 3$ *and* $s_0 \le m+2$,

$$\mathfrak{b} = \begin{cases} \mathfrak{p}^3, \ N(\mathfrak{p}) = 3, \ \textit{if} \ s_0 = m+1 & (2.2.4) \\ \mathfrak{p}, \ N(\mathfrak{p}) = 27, & \\ \qquad \textit{if} \ s_0 = m+2 \ \textit{and} \ D_3 \equiv (-1)^{m-1} (\textit{mod} \ 3) & (2.2.5) \\ \mathfrak{p}.\mathfrak{p}', \ N(\mathfrak{p}) = 3, N(\mathfrak{p}') = 9, & \\ \qquad \textit{if} \ s_0 = m+2 \ \textit{and} \ D_3 \equiv (-1)^{m} (\textit{mod} \ 3). & (2.2.5) \end{cases}$$

If $p > 3$ *or* $p = 3$ *and* $s_0 > m+2$,

$$\mathfrak{b} = \begin{cases} \mathfrak{p}_m^{e_m}.\mathfrak{p}^2, N(\mathfrak{p}_m) = N(\mathfrak{p}) = p, \ \textit{if} \ v_p(D) \ \textit{odd} & \\ \mathfrak{p}_m^{e_m}.\mathfrak{p}, N(\mathfrak{p}_m) = N(\mathfrak{p}) = p^2, \ \textit{if} \ v_p(D) \ \textit{even} & \\ \qquad \textit{and} \ \left(\dfrac{(-1)^{\frac{n(n-1)}{2}} 2D_p}{p} \right) = -1 & (2.2.6) \\ \mathfrak{p}_m^{e_m}.\mathfrak{p}.\mathfrak{p}', N(\mathfrak{p}_m) = N(\mathfrak{p}) = N(\mathfrak{p}') = p, \ \textit{otherwise} & \end{cases}$$

Moreover $I = J$ *in cases (2.2.2) and (2.2.4),* $I = J+1$ *in case (2.2.3) and* $I = J + [(s_0 - m)/2] + 1$ *in the rest of the cases.*

THEOREM 4. *Suppose that* $2|A$, $2 \not| B$ *and let* r_0, r_1, r, s_0, e, e_k $(1 \le k < m)$, J *and* I *be as in Theorem 3. Let* $u = [(s_0 - m + 1)/2]$. *Then we have*

$$(2.2.7) \quad 2 = \begin{cases} \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_{r-2}^{e_{r-2}}.\mathfrak{a}, & N(\mathfrak{p}_k) = 2 \ \textit{for all} \ k, \ \textit{if} \ r \le m, \\ \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_{m-2}^{e_{m-2}}.\mathfrak{b}, & N(\mathfrak{p}_k) = 2 \ \textit{for all} \ k, \ \textit{if} \ r = m+1, \end{cases}$$

where

$$\mathfrak{a} = \begin{cases} \mathfrak{p}^{e}, N(\mathfrak{p}) = 4, \quad if \ \ r_0 \leq r_1 & (2.2.8) \\ \mathfrak{p}_{m-1}^{e_{m-1}}\mathfrak{p}, N(\mathfrak{p}_{m-1}) = 2, N(\mathfrak{p}) = 4, if \ r_1 = m \ and \ r_0 = m+1 & (2.2.9) \\ \mathfrak{p}_{r-1}^{e_{r-1}}\mathfrak{p}^{e-1}\mathfrak{p}', \ N(\mathfrak{p}_{m-1}) = N(\mathfrak{p}) = N(\mathfrak{p}') = 2, \ otherwise & (2.2.9) \end{cases}$$

$$\mathfrak{b} = \begin{cases} \mathfrak{p}^2, N(\mathfrak{p}) = 2, if \ v_2(D) - m \ \ even \ or \\ \qquad\qquad D_2 \equiv 1 + 2^u (mod\ 4) & (2.2.10) \\ \mathfrak{p}, N(\mathfrak{p}) = 4, if \ \ v_2(D) - m \ odd \ and \\ \qquad\qquad D_2 \equiv 3 + n^u + 2^{u^2} (mod\ 8) & (2.2.11) \\ \mathfrak{p}.\mathfrak{p}', N(\mathfrak{p}) = N(\mathfrak{p}') = 2, if \ v_2(D) - m \ odd \ and \\ \qquad\qquad D_2 \equiv 7 + n^u + 2^{u^2} (mod\ 8) & (2.2.11) \end{cases}$$

Moreover $I = J$ *in cases* (2.2.8), $I = J + 1$ *in cases* (2.2.9), $I = J + u - 1$ *in cases* (2.2.10) *and* $I = J + u$ *in cases* (2.2.11).

2.3. Quartic and quintic trinomials

In this section we complete the general theorems above in the cases $n = 4$ and 5. Let $n = p^m$. Theorems 2, 3 and 4 give the decomposition of p in all cases except for the following :

(2.3.1) $$p | v_p(B) \ \text{ and } \ 0 < v_p(B) \leq v_p(A).$$

For the primes $q \neq p$ the only case not covered by Theorem 1 is :

(2.3.2) $$q | (n-1, v_q(A)) \ \text{ and } \ 0 < v_q(A) < v_q(B).$$

Equations satisfying (2.3.1) or (2.3.2) can be handled by an specific treatment but the results are too disperse to fit them into a reasonable theorem. For instance, for $n = 4$, (2.3.2) is not possible and (2.3.1) occurs only for $p = 2$ and equations :

(2.3.3) $$X^4 + 2^{2+e}AX + 2^2B, \ \ 2 \nmid AB, \ e \geq 0.$$

For $n = 5$, (2.3.1) is not possible and (2.3.2) occurs only for $q = 2$ and equations :

(2.3.4) $$X^5 + 2^2BX + 2^{3+e}C, \ \ 2 \nmid BC, \ e \geq 0.$$

THEOREM 5. *The decomposition of 2 in the number field defined by* (2.3.3) *or* (2.3.4) *is*

$$2 = \begin{cases} \mathfrak{a}, & if \ \ n = 4, \\ \mathfrak{r}\ \mathfrak{a}, \ \ N(\mathfrak{r}) = 2, \ \ \mathfrak{r} \not| \mathfrak{a}, & if \ n = 5, \end{cases}$$

where $\mathfrak{a}$ *is an integer ideal having the following decomposition :*

$$\mathfrak{a} = \mathfrak{p}^4, \quad if \quad e = 0 \ \ or \ \ 1.$$

For $e \geq 2$ *and* $B \equiv 1(mod\ 4)$ *:*

$$\mathfrak{a} = \begin{cases} \mathfrak{p}^4, if \ e = 2, B \equiv 1(mod\ 8) \ or \ e \geq 3, B \equiv 5(mod\ 8), \\ \mathfrak{p}^2\mathfrak{p}_1^2, if \ \ e = 2, B \equiv 13(mod\ 16) \ or \ e \geq 3, B \equiv 1(mod\ 16), & (2.3.5) \\ \mathfrak{p}_2^2, if \ e = 2, B \equiv 5(mod\ 16) \ or \ e \geq 3, B \equiv 9(mod\ 16). & (2.3.6) \end{cases}$$

Whereas for $e \geq 2$ *and* $B \equiv 3(mod\ 4)$ *:*

$$\mathfrak{a} = \begin{cases} \mathfrak{p}^2\mathfrak{p}_1^2, & if \ \ B \equiv 7(mod\ 8), \\ \mathfrak{p}_2^2, & if \ \ B \equiv 3(mod\ 8). \end{cases}$$

In all cases $N(\mathfrak{p}) = N(\mathfrak{p}_1) = 2$ *and* $N(\mathfrak{p}_2) = 4$. *Moreover,* $v_2(d) = 4$ *when* $e = 0$ *and in the cases* (2.3.5), (2.3.6) *and* $v_2(d) = 6$ *in the rest of the cases.*

3. Proofs

The proofs of the Theorems of Section 2 are essentially based on an old technique developed by Ore concerning Newton's polygon of the trinomial $f(X)$ (cf. [3] and [4]). For commodity of the reader we sum up the results we need of [3] and [4] in Theorem 6 below.

We recall first some definitions about Newton's polygon. Let $F(X) = X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$ and $p \in \mathbb{Z}$ be a prime number. The lower convex envelope Γ of the set of points $\{(i, v_p(a_i)), 0 \leq i \leq n\}(a_0 = 1)$ in the euclidean 2-space determines the so-called "Newton's polygon of $F(X)$ with respect to p". Let $S_1, \ldots, S_t$ be the sides of the polygon and ℓ_i, h_i the lenght of the projections of S_i to the X-axis and Y-axis respectively. Let $\varepsilon_i = (\ell_i, h_i)$ and $\ell_i = \varepsilon_i.\lambda_i$ for all i. If S_i begins at the point $(s, v_p(a_s))$ let $s_j = s + j\lambda_i$ and :

$$b_j = \begin{cases} (a_{s_j})_p & \text{if the point } (s_j, v_p(a_{s_j})) \text{ belongs to } S_i, \\ 0 & \text{otherwise,} \end{cases}$$

for all $0 \leq j \leq \varepsilon_i$. The polynomial :

$$F_i(Y) = b_0 Y^{\varepsilon_i} + b_1 Y^{\varepsilon_i - 1} + \cdots + b_{\varepsilon_i},$$

is called the "associated polynomial of S_i". We define $F(X)$ to be "S_i-regular" if p does not divide the discriminant of $F_i(Y)$. $F(X)$ will be called "Γ-regular" if it is S_i-regular for all i.

THEOREM 6. (Ore [4], Theorems 6 and 8). *Let $F(X) \in \mathbb{Z}[X]$ be a monic irreducible polynomial and let $L = \mathbb{Q}(\alpha)$, α a root of $F(X)$. Let $p \in \mathbb{Z}$ be a prime ; with the above notations about Newton's polygon Γ of $F(X)$ with respecto to p, we have the following decomposition of p into a product of integer ideals of L :*

$$p = \mathfrak{a}_1^{\lambda_1} \cdot \ldots \cdot \mathfrak{a}_t^{\lambda_t}.$$

For each i, the ideal $\mathfrak{a}_i$ is p-analogous to $F_i(Y)$ if $F(X)$ is S_i-regular. Moeover, if $F(X)$ is Γ-regular we have :

$$v_p(i(\alpha)) = \sum_{i=2}^{t} \ell_i \left(\sum_{j=1}^{i-1} h_j \right) + \frac{1}{2} \sum_{i=1}^{t} (\ell_i h_i - \ell_i - h_i + \varepsilon_i),$$

where $i(\alpha)$ denotes the index of α. This expression for $v_p(i(\alpha))$ also coincides with the number of points with integer coordinates below the polygon except for the points on the X-axis and on the last ordinate.

For the proof of theorem 1 we need a well-known lemma (cf.[5]) :

LEMMA 1. *Let L be a number field of degree $[L : \mathbb{Q}] = n$. Let q be a prime integer unramified in L and let s be the number of prime ideals of L lying over q. Then, the discriminant d of L satisfies*

$$\left(\frac{d}{q} \right) = (-1)^{n-s}.$$

Proof of theorem 1. The assertions (2.1.1) and (2.1.2) are a straightforward application of Theorem 6. For (2.1.3) see the proof of [2 Theorem 2]. (2.1.4) is consequence of Lemma 1 and the fact that in this case $v_q(d) = 1$ if q ramifies [2, Theorem 2]. (2.1.5) is obvious and the assertions concerning the computation of $v_q(d)$ are contained in [2, Theorem 1].

Theorem 2 follows from Theorem 6 and [2, Theorem 1]. We shall deal with the proof of Theorems 3 and 4 altogether. The proof of Theorem 5 is similar to those of the general theorems.

Proof of Theorem 3 and 4. Since $p|A$ and $p \not| B$, we have $f(X) \equiv (X+B)^n \pmod p$. Let Γ be the Newton's polygon of the polynomial :

$$F(X) := f(X-B) = \sum_{i=0}^{n} A_i X^{n-i},$$

where $A_0 = 1$, $A_i = \binom{n}{i}(-B)^i$ for $1 \le i \le n-2$, $A_{n-1} = f'(-B)$ and $A_n = f(-B)$.

It is easy to see that :

$$(3.2.1) \qquad v_p(A_i) = v_p(\binom{n}{i}) = m - v_p(i), \quad 1 \le i \le n-2.$$

Let us determine first which would be the partial shape of Γ if the two final points $(n-1, r_1), (n, r_0)$ where omitted. By (3.2.1) we find that in that case Γ would have $m-1$ sides $S_1, \dots, S_{m-1}$ if $p = 2$ and one more side S_m if $p > 2$, each side S_k ending at the point (e_k, k) (see figure 1). In fact, $i = e_k$ is the greatest subindex with $v_p(A_i) = k$ and the slope of S_k is $1/e_k$ so that these slopes are stictly increasing. Now, when we consider the two final points of Γ we find that we can always assure that Γ contains the sides $S_1, \dots, S_{m-1}$ if $r > m$, the sides $S_1, \dots, S_{r-1}$ if $r \le m$ and $p > 2$, and the sides $S_1, \dots, S_{r-2}$ if $r \le m$ and $p = 2$.

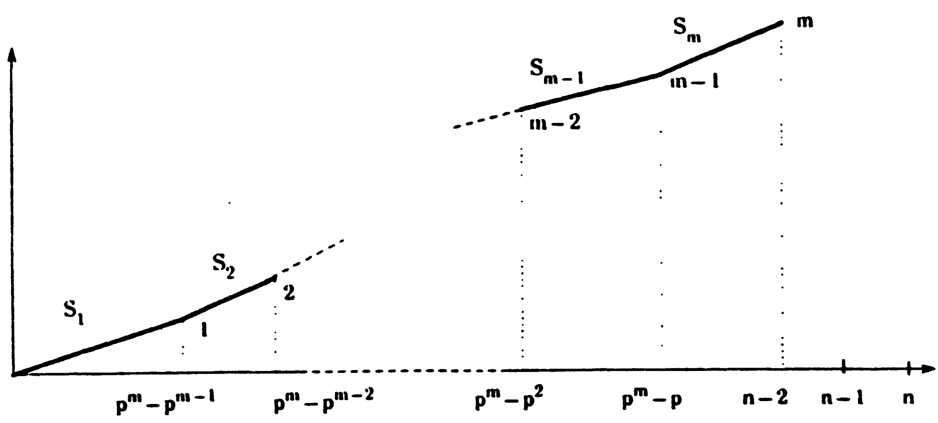


Figure 1

Let Γ' denote, in each case, the rest of the sides of Γ. By Theorem 6, the assertions (2.2.1) and (2.2.7) are proved. In order to find the further decomposition of the respective ideals $\mathfrak{a}$ and $\mathfrak{b}$ of Theorem 3 and 4 we shall study the shape and associated polynomials of Γ'. We must distinguish several cases. Before, note that for each $1 \le k \le m$, the number of points with integer coordinates below the sides $S_1 \cup \cdots \cup S_k$ except for the points on the X-axis and on the last ordinate is

$$I_k = p^{m-k}\left(\frac{p^k - 1}{p-1} - k\right) \quad \text{for } 1 \le k < m,$$

and

$$I_m = \frac{n-1}{p-1} - 2m + 1.$$

Case $r \le m, r_0 \le r_1$: Γ' has only one side with lengths of the projections to the axis : $\ell = p^{m-r_0+1} = e,\ h = 1$ if $p > 2$ and $\ell = 2e,\ h = 2$ if $p = 2$ (see fig. 2). Therefore $\varepsilon := (\ell, h) = 1$ or 2 according to $p > 2$ or $p = 2$. In the latter case the associated polynomial is congruent (mod 2) to $Y^2 + Y + 1$, which is irreducible. By Theorem 6, (2.2.2) and (2.2.8) are proved. Since $F(X)$ is Γ-regular we have :

$$\begin{aligned} I &= I_{r-1} + e(r-1) && \text{if } p > 2, \\ I &= I_{r-2} + e(2r-3) && \text{if } p = 2, \end{aligned}$$

hence, $I = J$ in both cases, as desired.

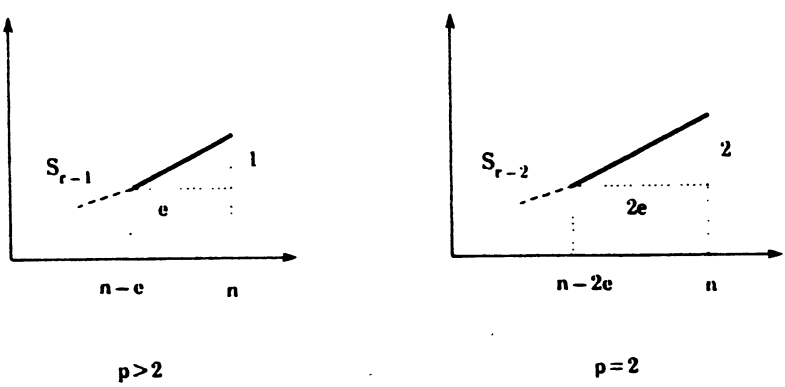


Figure 2

Case $r \leq m, r_0 > r_1$: If $p > 2$, Γ' has two sides S, S' with projections to the axis $\ell = e - 1, h = 1$ and $\ell' = 1, h' = r_0 - r_1$ respectively (see fig. 3). If $p = 2$, Γ' contains the side S_{r-1} and two more sides with the same dimensions of S and S' above, except for the case $r_1 = m, r_0 = m + 1$ in which besides S_{m-1} there is only one side with projections to the axis $\ell = h = 2$ and associated polynomial congruent (mod 2) to $Y^2 + Y + 1$, which is irreducible (see fig. 3). By Theorem 6, (2.2.3) and (2.2.9) are proved. Since $F(X)$ is Γ-regular in any case, we have :

$$I = I_{m-1} + 2m - 1 \qquad \text{if } p = 2, r_1 = m \text{ and } r_0 = m + 1,$$
$$I = I_{r-1} + e(r - 1) + 1 \qquad \text{otherwise ,}$$

hence $I = J + 1$ in both cases, as desired.

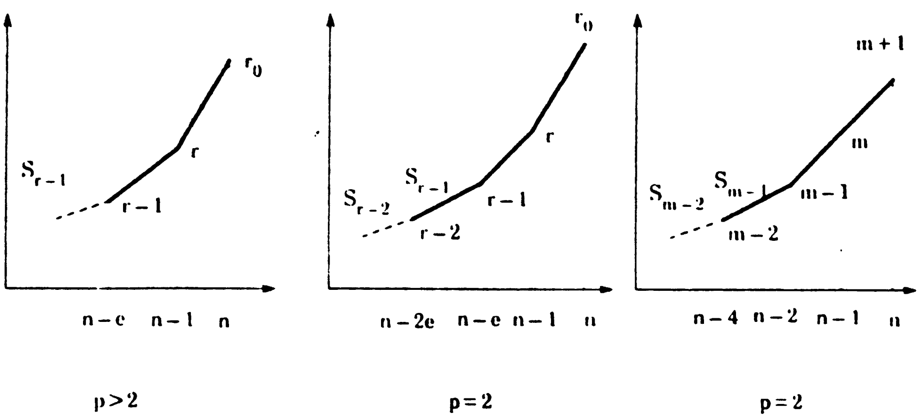


Figure 3

This ends the discusion of the case $r \leq m$.

Assume from now on that $r = m + 1$. If we study Γ' in this case as above, we are led to many p-irregular cases. For this reason, instead of the polynomial $f(X - B)$ we seek an opportune substitute providing a much more regular situation.

Since $r_1 = v_p(n(-B)^{n-1} + A) > m$, we have :

$$v_p(A) = m \quad \text{and } A_p \equiv -1(\text{mod} p).$$

Thus, from $r_0 = v_p((-B)^{n-1} + A - 1) > m$, we get :

(3.2.2.) $$(-B)^{n-1} \equiv 1 + p^m (\text{mod } p^{m-1}).$$

Let $\beta = -nB/(n-1)A$. Since $v_p(\beta) = 0$, β is a p-adic integer and it is clear that Theorem 6 is also applicable to the polynomial :

$$G(X) := f(X+\beta) = \sum_{i=0}^{n-2} \binom{n}{i} \beta^i X^{n-i} + f'(\beta)X + f(\beta).$$

Computation leads to :

$$f(\beta) = (-1)^{\frac{n(n+1)}{2}} \frac{BD}{(n-1)^n A^n}, f'(\beta) = (-1)^{\frac{n(n+1)}{2}-1} \frac{D}{(n-1)^{n-1}A^{n-1}},$$

hence, $s_0 := v_p(f(\beta)) = v_p(D) - nm$ and $s_1 := v_p(f'(\beta)) = s_0 + m$. It is easy to check that :

$$A_p^n \equiv (-1)^n \text{ (mod } p^{m+1}) \text{ and } (n-1)^{n-1} \equiv (-1)^{n-1}(1+n) \text{ (mod } p^{m+1}),$$

hence, by (3.2.2) :

$$\frac{(-1)^{\frac{n(n-1)}{2}} D}{n^n} = B^{n-1} + (-1)^{n-1}(n-1)^{n-1} A_p^n \equiv 0 \text{ (mod } p^{m+1}),$$

so that $s_0 = v_p(D/n^n) > m$. Thus, Newton's polygon Γ_β of $G(X)$ with respect to p can be also expressed as :

$$\Gamma_\beta = S_1 \cup \cdots \cup S_{m-1} \cup \Gamma'_\beta,$$

and we need only to study Γ'_β in order to find the prime-ideal decomposition of the respective ideals $\mathfrak{b}$ of Theorems 3 and 4. Again, we have to distinguish several cases :

Case $r = m+1, p > 3$ *or* $p = 3$ *and* $s_0 > m+2$: Γ'_β contains S_m and one more side of dimensions $\ell = 2, h = s_0 - m$ (see fig. 4). For this latter side, $\varepsilon = (\ell, h) = 1$ or 2 according to $s_0 - m$ odd or even. In the latter case the associated polynomial is :

$$\frac{n-1}{2}\beta^{n-2}Y^2 + \frac{f(\beta)}{p^{s_0}}$$
$$\equiv \frac{B^{n-2}}{2} Y^2 + (-1)^{\frac{n(n+1)}{2}} BD_p (\text{mod } p),$$

and its discriminant is congruent to $(-1)^{n(n-1)/2}2D_p$. Since $v_p(D) \equiv s_0 - m \pmod 2$, (2.2.6) is proved by Theorem 6, Moreover, since we are in a regular case we have :

$$I = I_m + 2m - 1 + \frac{s_0 - m + \varepsilon}{2} = J + \left[\frac{s_0 - m}{2}\right] + 1,$$

as desired.

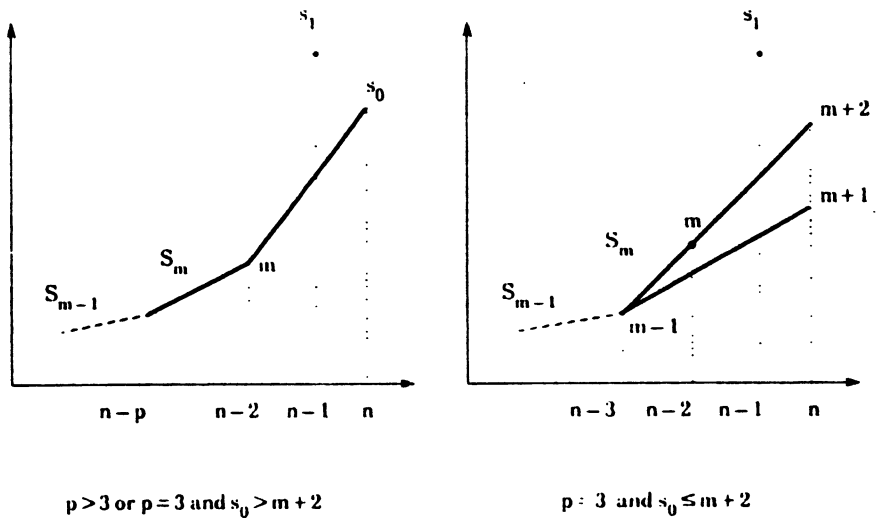


Figure 4

Case $r = m + 1, p = 3$ *and* $s_0 \leq m + 2$: Γ'_β has only one side with $\ell = 3$ and $h = 2$ or 3 according to $s_0 = m + 1$ or $m + 2$ (see fig. 4). In the latter case $\varepsilon = 3$ and the associated polynomials is

$$\frac{(n-1(n-2)}{2}\beta^{n-3}Y^3 + \frac{n-1}{2}\beta^{n-2}Y^2 + \frac{f(\beta)}{3^{s_0}}$$
$$\equiv B^{n-3}Y^3 - B^{n-2} + (-1)^{m-1}BD_3 \pmod 3.$$

Since $(-1)^{n(n+1)/2} = (-1)^{m-1}$ in this case, multiplying by B^2 we get the polynomial $\Phi(Y) = Y^3 - By^2 + (-1)^{m-1}BD_3$, which is irreducible (mod 3) if $D_3 \equiv (-1)^{m-1} \pmod 3$ and factorizes :

$$\phi(Y) \equiv (Y + B)(Y^2 + BY - 1) \pmod 3,$$

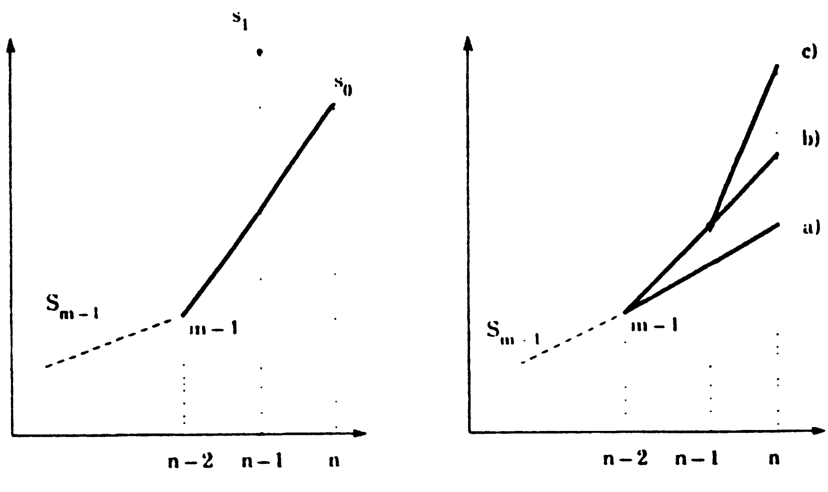
if $D_3 \equiv (-1)^m \pmod 3$. By Theorem 6, (2.2.5) is proved. Since we are in a regular case we have :

$$I = I_{m-1} + 3m - 2 = J \quad \text{if} \quad s_0 = m + 1,$$
$$I = I_{m-1} + 3m = J + 2 \quad \text{if} \quad s_0 = m + 2.$$

Case $r = m+1, p = 2$: Γ'_β has only one side with $\ell = 2$ and $h = s_0 - m + 1$ (see fig.5), hence $\varepsilon = 1$ or 2 according to $s_0 - m + 1$ odd or even, or equivalently according to $v_2(D) - m$ even or odd. In the latter case, the associated polynomial is congruent (mod 2) to $Y^2 + 1$, hence, it is an irregular case. In the former case Theorem 6 proves (2.2.10) and :

$$I = I_{m-1} + 2m - 2 + \frac{s_0 - m}{2} = J + u - 1,$$

as desired.



p = 2 and s_0 − m + 1 odd   p = 2 and s_0 − m + 1 even

Figure 5

Finally, in order to deal with the case $v_2(D) - m$ odd it is necessary to change again Newton's polygon. Let $2u = s_0 - m + 1$ and $\delta = (2^u - B)/(n-1)A_2$. Computation leads to :

$$(3.2.3) \qquad (n-1)^n A_2^n f(\delta) = \sum_{i=0}^{n-2} \binom{n}{i} 2^{(n-i)u} (-B)^i + (B - 2^{u+m}) D_0,$$

where $D_0 = D/n^n = B^{n-1} - (n-1)^{n-1}A_2^n$. Since $v_2(D_0) = s_0 = 2u + m - 1 > m, u > 0$ and there are exactly two summands in (3.2.3) with v_2 minimum and equal to $2u + m - 1$, hence, $v_2(f(\delta)) \geq 2u + m$. From the relation :

$$nf(X) - Xf'(X) = (n-1)AX + nB,$$

and being $v_2((n-1)A\delta + nB) = u + m$, we conclude that $v_2(f'(\delta)) = u + m$. Thus Newton's polygon Γ_δ with respect to p of the polynomial $f(X + \delta)$ is again expressible as : $\Gamma_\delta = S_1 \cup \cdots \cup S_{n-1} \cup \Gamma'_\delta$. We have now three possibilities (see fig.5) :

a) $v_2(f(\delta)) = 2u + m$. Γ'_δ has only one side with $\ell = 2$, $h = 2u + 1$ hence $\varepsilon = (\ell, h) = 1$ and $\mathfrak{a} = \mathfrak{p}^2, N(\mathfrak{p}) = 2$. Moreover $I = I_{m-1} + 2(m-1) + u = J + u - 1$.

b) $v_2(f(\delta)) = 2u + m + 1$. Γ'_δ has only one side with associated polynomial congruent (mod 2) to $Y^2 + Y + 1$, which is irreducible, hence $\mathfrak{a} = \mathfrak{p}, N(\mathfrak{p}) = 4$. Moreover $I = I_{m-1} + 2(m-1) + u + 1 = J + u$.

c) $v_2(f(\delta)) > 2u + m + 1$. Γ'_δ has two sides and $\mathfrak{a} = \mathfrak{p}.\mathfrak{p}'$, $N(\mathfrak{p}) = N(\mathfrak{p}') = 2, I = J + u$ like in case b).

Taking congruence (mod 2^{2u+m+2}) of (3.2.3) we shall be able to decide in which case falls our polynomial. All summands of (3.2.3) vanish (mod 2^{2u+m+2}) except for the following :

$$\binom{n}{4} 2^{4u}(-B)^{n-4} + \binom{n}{3} 2^{3u}(-B)^{n-3} + \binom{n}{2} 2^{2u}(-B)^{n-2} + BD_0.$$

Dividing by 2^{2u+m+1} and taking congruence (mod 8) we obtain :

(3.2.4) $$2^{2u+m+1} - 2^{2u-1} + 2^{u+1} + 2^m - 1 + BD_2 \pmod 8$$

From (3.2.2) we get $B \equiv -1 + 2^m \pmod{2^{m+1}}$, hence (3.2.4) is equal to :

$$2^{2u+m-2} - 2^{2u-1} + 2^{u+1} - 1 - D_2 \pmod 8$$

which is equal to $-1 - D_2$ (mod 8) if $u > 1$ and to $2^m + 1 - D_2$ if $u = 1$. Therefore cases a) b) and c) are equivalent to the following respective conditions :

$$a) \Leftrightarrow \begin{cases} D_2 \equiv 1 \pmod 4 & \text{if } u > 1 \\ D_2 \equiv -1 \pmod 4 & \text{if } u = 1 \end{cases}$$

$$b) \Leftrightarrow \begin{cases} D_2 \equiv 3 \pmod 8 & \text{if } u > 1 \\ D_2 \equiv 5 + n \pmod 8 & \text{if } u = 1 \end{cases}$$

$$c) \Leftrightarrow \begin{cases} D_2 \equiv -1 \pmod 8 & \text{if } u > 1 \\ D_2 \equiv 1 + n \pmod 8 & \text{if } u = 1 \end{cases}$$

This ends the proof of (2.2.10) and (2.2.11).

REFERENCES

[1] P. Llorente - E. Nart, *Effective determination of the decomposition of the rational primes in a cubic field*, Proc. Amer. Math. Soc. **87** (1983), 579-585.

[2] P. Llorente - E. Nart - N. Vila, *Discriminants of number fields defined by trinomials*, Acta Arith. **43** (1984), 367-373.

[3] Ö. Ore, *Zur Theorie der algebraischen Körper*, Acta Math. **44** (1923), 219-314.

[4] Ö. Ore, *Newtonsche Polygone in der Theorie des algebraischen Körper*, math. Ann. **99** (1928), 84-117.

[5] R. G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. **12** (1962), 1099-1106.

[6] W. Y. Vélez, *The factorization of p in* $\mathbb{Q}(a^{1/p^k})$ *and the genus field of* $\mathbb{Q}(a^{1/n})$, Tokyo J. Math. **11** (1988), 1-19.

Dept. Matemàtiques
Univ. Autònoma de Barcelona
08193 Bellaterra, Barcelona
Spain.

Dept. Àlgebra i Geometria
Facultat de Matemàtiques
Univ. de Barcelona
Gran Via, 585
08007 Barcelona
Spain.